

FILEDUNITED STATES DISTRICT COURT
ALBUQUERQUE, NEW MEXICO

UNITED STATES DISTRICT COURT

for the
District of New Mexico

JUL 30 2018

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Information associated with the cellular device assigned
with call number 505-582-4555 that is in the custody or
control of T-Mobile.

Case No.

18mr667

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the _____ District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1201(a)(1)	Kidnapping
18 U.S.C. § 2119	Carjacking
18 U.S. Code § 1951	Interference with Commerce by Threats or Violence (Hobbs Act)

The application is based on these facts:
See attached affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I certify that the requested records
and information are relevant to an ongoing
criminal investigation.

Sworn to before me and signed in my presence.

Date:

7/27/18

Jack Burkhead
Assistant U.S. AttyCity and state: Albuquerque, New Mexico

Applicant's signature

Daniel Fondse, Special Agent - FBI

Printed name and title

Judge's signature

Steven C. Yarbrough

Printed name and title

U.S. Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR DEVICE ASSIGNED WITH
CALL NUMBER 505-582-4555 THAT IS IN
THE CUSTODY OR CONTROL OF T-
MOBILE

Case No. _____

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Daniel Fondse, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular device assigned with call number 505-582-4555 (“the SUBJECT ACCOUNT”), with listed subscriber(s) Jose Ramirez, that is in the custody or control of T-Mobile, a wireless communications service provider that is headquartered at 4 Sylvan Way, Parsippany, NJ 07054. As a provider of wireless communications service, T-Mobile is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15).

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 to require T-Mobile to disclose to the government the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

3. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. *See* 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. *See* 18 U.S.C. § 3123(b)(1).

4. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed since May 2017. I am therefore authorized to investigate federal criminal offenses. I am currently a member of the Violent Crimes Squad of the Albuquerque Division of the FBI. I have received on the job training from other experienced agents and detectives in the investigations of violent crimes. Prior to joining the FBI, I spent three years as a sworn law enforcement officer of the San Diego Police Department. My investigative training and experience includes, but is not limited to, conducting surveillance, interviewing subjects, victims, and witnesses, writing affidavits for and executing search and arrest warrants, managing cooperating sources, issuing subpoenas, collecting evidence, and analyzing public records. I also received both Bachelor and Master of Science degrees in Mechanical Engineering.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1201(a)(1) - Kidnapping, 18 U.S.C. § 2119 - Carjacking, 18 U.S. Code § 1951 - Interference with Commerce by Threats or Violence (Hobbs Act), 18 U.S.C. § 371 -

Conspiracy, and 18 U.S.C. § 2 - Aiding and Abetting have been committed by Jose Ramirez.

There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes as further described in Attachment B.

7. The Court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated.

PROBABLE CAUSE

8. The United States, including the Federal Bureau of Investigation, is conducting a criminal investigation of Jose Ramirez regarding possible violations of 18 U.S.C. § 1201(a)(1) - Kidnapping, 18 U.S.C. § 2119 - Carjacking, 18 U.S. Code § 1951 - Interference with Commerce by Threats or Violence (Hobbs Act), 18 U.S.C. § 371 - Conspiracy, and 18 U.S.C. § 2 - Aiding and Abetting.

9. On July 26, 2018 a kidnapping was reported to the Federal Bureau of Investigations (FBI), Albuquerque Division. The reporting party stated they were unable to locate or contact the victim, a family member. The reporting party stated they received approximately five phone calls on July 26, 2018 from person(s) alleging to have kidnapped the victim and who demanded money from the reporting party. The phone number(s) used to place the calls to the reporting party were blocked. By analyzing cellular phone records obtained through exigent circumstances, FBI personnel determined the SUBJECT ACCOUNT placed five phone calls on July 26, 2018 to the reporting party, which corresponded to the times the reporting party was contacted by the alleged kidnapper(s). T-Mobile records show the subscriber of the SUBJECT ACCOUNT is Jose Ramirez, the subscriber address is 10317 Jenaro St SW, Albuquerque, NM 87121 and the subscriber name effective date was July 03, 2018. The

kidnapping victim later stated Jose Ramirez was known to them. Ramirez is currently the subject of an active federal arrest warrant issued on July 27, 2018 for alleged violation of 18 U.S.C. § 1201(a)(1) - Kidnapping, 18 U.S.C. § 2119 - Carjacking, 18 U.S. Code § 1951 - Interference with Commerce by Threats or Violence (Hobbs Act), 18 U.S.C. § 371 - Conspiracy, and 18 U.S.C. § 2 - Aiding and Abetting in relation to the previously described incidents. Due to the nature of the offenses he may be aware of the law enforcement investigation into this incident and may be taking active measures to avoid law enforcement. As such, it may take significant time and resources to locate Jose Ramirez, establishing probable cause to monitor the SUBJECT ACCOUNT for up to 45 days after the alleged kidnapping.

10. Your Affiant knows from his training and experience that criminals frequently use electronic devices, such as cellular phones, to coordinate and promote criminal acts. These communications can be in the form of calls, text messages or messaging applications built into the social media platforms including photographs, or videos. Electronic communication can be used to coordinate with accomplices or for such purposes as making logistical arrangements, arranging transportation, or disposing of evidence. Your Affiant knows from experience, most people carry a cellular phone on their person at all times. Information regarding the locations and communications associated with the cellular telephone are often useful and relevant as evidence in criminal investigations.

11. There is also probable cause to believe that the locations related to the SUBJECT ACCOUNT will assist Law Enforcement in arresting Jose Ramirez pursuant to his active warrant. Historical information from the SUBJECT ACCOUNT will likely provide Law

Enforcement with information relevant to the investigation of the previously described kidnapping during which the SUBJECT ACCOUNT was utilized.

12. In my training and experience, I have learned that T-Mobile is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the “sector” (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

13. Based on my training and experience, I know that T-Mobile can collect cell-site data on a prospective basis about the SUBJECT ACCOUNT. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as T-Mobile typically collect and retain cell-site data pertaining to cellular devices to which

they provide service in their normal course of business in order to use this information for various business-related purposes.

14. Based on my training and experience, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), a Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Equipment Identity (“IMEI”). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication’s content.

15. Based on my training and experience, I know that wireless providers such as T-Mobile typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as T-Mobile typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the SUBJECT ACCOUNT's user or users and may assist in the identification of co-conspirators and/or victims

AUTHORIZATION REQUEST

16. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41. The proposed warrant will also function as a pen register order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and/or trap and trace device to record, decode, and/or capture certain information in Attachment A for each communication to or from the SUBJECT ACCOUNT, without geographic limit, for a period of forty-five days (45) days pursuant to 18 U.S.C. § 3123(c)(1).

17. I further request that the Court direct T-Mobile to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on T-Mobile, who will then compile the requested

records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

18. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully submitted,



Daniel Fondse
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on July 27, 2018


UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular device assigned call number 505-582-4555 that is in the custody or control of T-Mobile, a wireless communications service provider that is headquartered at 4 Sylvan Way, Parsippany, NJ 07054.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

- a. The following information about the customers or subscribers associated with the SUBJECT ACCOUNT for the time period of 60 days:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");
 - vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

- viii. Means and source of payment for such service (including any credit card or bank account number) and billing records and
- ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the SUBJECT ACCOUNT, including:
 - (A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
 - (ii) information regarding the cell tower and antenna face (also known as “sectors” through which the communications were sent and received)

b. Information associated with each communication to and from the SUBJECT ACCOUNT for a period of 45 days from the date of this warrant, including:

- i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;
- ii. Source and destination telephone numbers;
- iii. Date, time, and duration of communication; and
- iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the SUBJECT PHONE will connect at the beginning and end of each communication.

II. Information to be Seized by the Government

All information described above in Section I that constitutes [evidence, fruits, contraband, and instrumentalities] of violations of 18 U.S.C. § 1201(a)(1) - Kidnapping, 18 U.S.C. § 2119 - Carjacking, 18 U.S. Code § 1951 - Interference with Commerce by Threats or

Violence (Hobbs Act), 18 U.S.C. § 371 - Conspiracy, and 18 U.S.C. § 2 - Aiding and Abetting involving Jose Ramirez **or** during the period **May 29, 2018 to September 10, 2018**.